CLAIMS

1. A method for a network node, which includes a central processing unit (CPU) configured to execute a router operating system, to filter malicious data packets received at the network node, the method comprising:

receiving a data packet at the network node;

performing hash-based flow classification on the received data packet to determine whether the received data packet is a malicious data packet; and

discarding the received data packet before the data packet can be forwarded to the CPU for processing by the router operating system, if the received data packet is determined to be a malicious data packet.

2. The method of claim 1, wherein the step of performing hash-based flow classification further comprises:

identifying a packet type associated with the received data packet;

extracting a set of signature information corresponding to the identified packet type; and

searching a hash table to locate the extracted set of signature information.

3. The method of claim 2, further comprising:

configuring the hash table, either manually or automatically, to associate the set of signature information with a data flow; and

determining whether the data flow associated with the set of signature information corresponds to a malicious data flow.

4. The method of claim 1, further comprising:

associating the received data packet with a destination in the network node as a result of the hash-based flow classification.

5. The method of claim 4, further comprising:

determining whether the destination associated with the received data packet is a predetermined destination associated with malicious data packets.

6. The method of claim 5, further comprising:

in response to determining that the destination associated with the received data packet is the predetermined destination, performing the steps of:

removing buffer pointers from a set of descriptors associated with the received data packet; and

storing the removed buffer pointers on a queue of free buffer pointers.

7. The method of claim 6, further comprising:

if the queue of free buffer pointers does not contain enough available entries to store the removed buffer pointers, storing the set of descriptors associated with the received data packet on a delete queue until enough entries become available in the queue of free buffer pointers.

8. The method of claim 6, further comprising:

transferring free buffer pointers from the router operating system to the queue of free buffer pointers.

9. The method of claim 1, wherein the step of performing hash-based flow classification is used in conjunction with an access control list or an intrusion detection system.

10. The method of claim 1, wherein the network node is an intermediate network node.

11. A network node, comprising:

a central processing unit (CPU) configured to execute instructions that implement a router operating system;

a network interface adapted to receive a data packet;

a memory having a plurality of storage locations addressable by the CPU, the storage locations being configured to store:

(i) at least a portion of the router operating system instructions,

(ii) one or more data buffers for storing the received data packet, and

(iii) a searchable data structure configured to store information associated with the received data packet; and

a system controller coupled to the memory and the CPU, the system controller including a hardware assist (HWA) module configured to discard malicious data packets from the network node before the malicious data packets can be forwarded to the CPU for processing by the router operating system.

12. The network node of claim 11, wherein the searchable data structure is a hash table.

13. The network node of claim 11, wherein the HWA module includes a direct memory access (DMA) controller and a flow classifier.

14. The network node of claim 13, wherein the DMA controller includes:

an ingress descriptor first in, first out (FIFO) queue configured to store a set of descriptors referencing the one or more data buffers in which the received data packet is stored;

a packet-header buffer configured to store information contained in at least one packet header prepended to the received data packet;

an egress descriptor FIFO configured to store the set of descriptors as well as a data flow identification (ID) value for identifying the data flow associated with the received data packet and a destination value for identifying a destination in the network node associated with the received data packet, the flow classifier searching the searchable data structure to locate the data flow ID value and the destination value; and

a free-buffer FIFO containing a set of free buffer descriptors allocated for the network interface.

15. The network node of claim 13, wherein the flow classifier includes:

a packet-identifier engine configured to identify a packet type associated with the received data packet based on information received from the DMA controller;

a signature-extraction engine configured to extract a set of signature information from a predetermined set of fields in the information received from the DMA controller, the predetermined set of fields being selected based on the packet type identified by the packet-identifier engine;

an address generator configured to generate a memory address based on the set of signature information, the memory address corresponding to an entry in the searchable data structure; and

a search module configured to search the searchable data structure to locate a flow ID value and a destination value associated with the received data packet.

16. The network node of claim 15, wherein the flow classifier further includes:

an egress packet manager configured to reformat descriptors from an ingress descriptor format to an egress descriptor format.

17. The network node of claim 11, wherein the network node is an intermediate network node.

18. A network node including a central processing unit (CPU) configured to execute a router operating system, the network node comprising:

means for receiving a data packet at the network node;

means for performing hash-based flow classification on the received data packet to determine whether the received data packet is a malicious data packet; and

means for discarding the received data packet before the data packet can be forwarded to the CPU for processing by the router operating system, if the received data packet is determined to be a malicious data packet.

19. A computer-readable media including instructions for execution by a processor, the instructions for a method of filtering malicious data packets received at a network node in which a central processing unit (CPU) is configured to execute a router operating system, the method comprising:

receiving a data packet at the network node;

performing hash-based flow classification on the received data packet to determine whether the received data packet is a malicious data packet; and

discarding the received data packet before the data packet can be forwarded to the CPU for processing by the router operating system, if the received data packet is determined to be a malicious data packet.